COSMOS
Navigate the Compliance Universe

Compliance Today - July 2021
Telehealth and HIPAA compliance during the pandemic and beyond

By Lakshmi Nathan, MS, MBA, CDPSE

Lakshmi Nathan (lakshmi.nathan@kp.org) is Senior Compliance Program Manager at Kaiser Permanente in Oakland, CA.

- linkedin.com/in/lakshmi-nathan/

The pandemic has had a significant impact on our lives. Zoom meetings, online classes, cancelled vacations, and virtual get-togethers have become the new normal. The pandemic has been a big challenge for the healthcare industry, too. During the early months of the pandemic, in-person visits to ambulatory practices decreased by nearly 60%.[1] Hospitals and providers were also forced to innovate rapidly to handle various challenges, from facing a shortage of personal protective equipment (PPE) to dealing with the surge of COVID-19 patients. To address these challenges, hospitals and providers adopted new technologies in a matter of weeks, something that usually took several years in the past. Social distancing and shelter-at-home policies forced providers to use telehealth as the primary mode of interaction with patients. Patients embraced telehealth services, too, because it provided a safer alternative to in-person visits.

What is telehealth?

A video call with our doctor is the image most of us have when we think of telehealth. Telehealth is more than video consultation. Telehealth modalities include live videoconferencing, remote patient monitoring, healthcare, and education provided through mobile device and sharing of health records electronically between healthcare professionals.

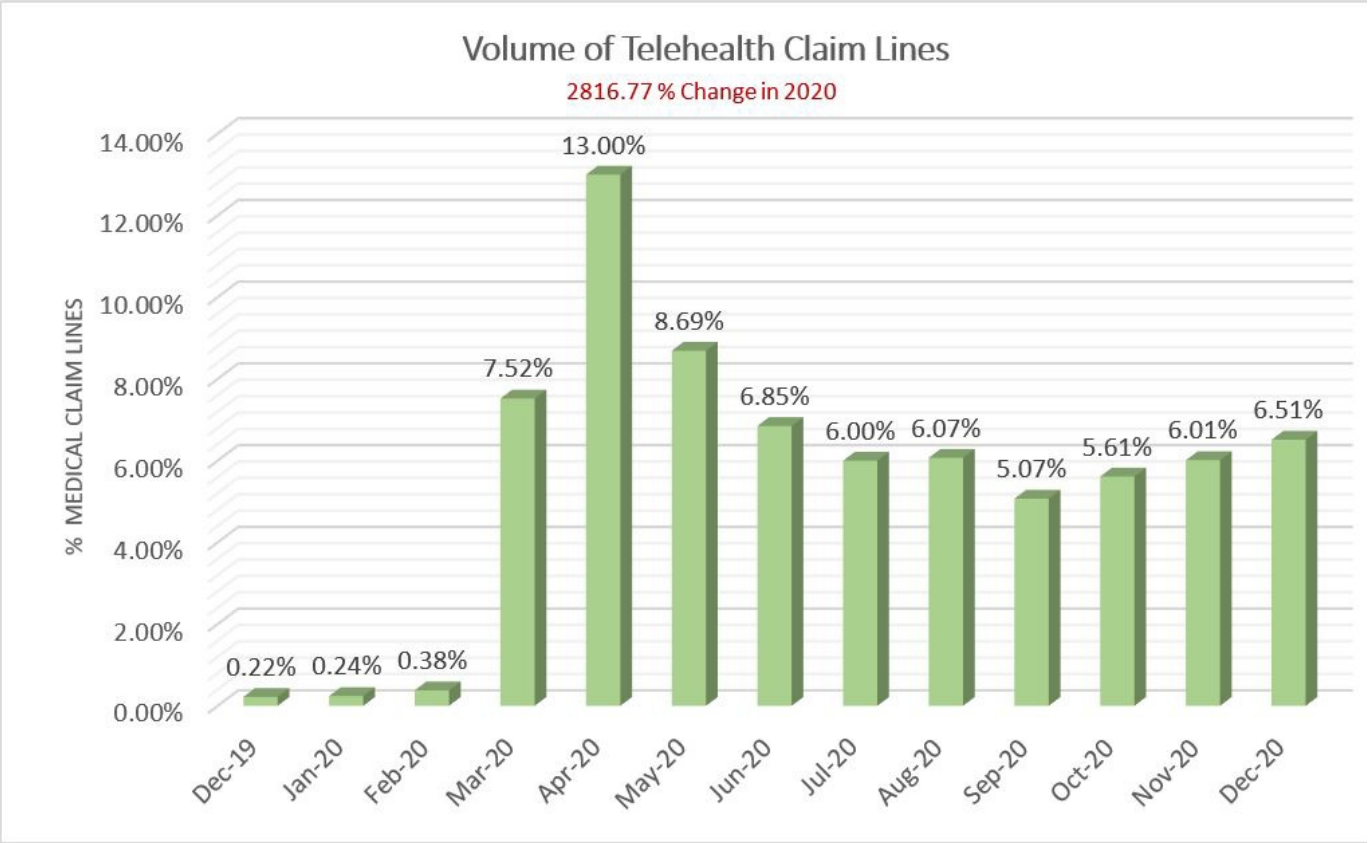
People also use the terms telemedicine and telehealth interchangeably, but they are different. Telemedicine refers to clinical services like diagnosis, consultation, treatment, etc. offered remotely, usually in real time by a licensed practitioner. Telehealth is a broader term that includes telemedicine and more. Telehealth refers to all healthcare interactions done remotely, including clinical services and nonclinical services like provider training, public health activities, etc.

Rapid adoption of telehealth during the pandemic

During the pandemic, US federal government enacted policies that encouraged adoption of telehealth services. On March 17, 2020, the U.S. Department of Health & Human Services (HHS) enacted policies like increasing patient populations eligible for telehealth, expanding coverage and reimbursement policies, increasing providers eligible for telehealth, and relaxing the Health Insurance Portability and Accountability Act (HIPAA) regulations to allow adoption of commercially available technologies for video visits.[2]

The unprecedented innovation combined with the HHS policy changes dramatically increased the use of telehealth. From December 2019 to December 2020, the volume of telehealth claim lines increased 2,816.77% nationally.[3] A claim line is an individual service or procedure listed on an insurance claim.

Figure 1: Volume of telehealth claim lines in 2020



What limited the widespread use of telehealth before the pandemic?

In 2013, the US federal government updated HIPAA to allow technology companies like Google, Apple, Skype, etc. to be treated as business associates of doctors and insurers.[4] To be HIPAA compliant, these companies were required to store and share patient data in a safe and secure way.

While the law allowed tech companies to be part of telehealth services, it also required them to go through several steps to be HIPAA compliant. For example, the tech companies and their subcontractors were required to enter into a business associate agreement with every doctor or practice using their technology. These contracts also required the tech companies to address several other requirements to be HIPAA complaint.

Before the pandemic, Medicare paid doctors and hospitals for telehealth only in limited circumstances, such as for appointments in specific rural areas or to treat specific conditions. In addition to HIPAA, providers also had to comply with various state-specific telehealth requirements. All these factors limited widespread use of telehealth.

HIPAA compliance waivers for telehealth technology during the pandemic

The HHS Office for Civil Rights issued a notification of enforcement discretion to allow healthcare providers to use available communication applications without the risk of penalties for HIPAA violations for telehealth services.[5]

Under this notice, healthcare providers were allowed to deliver telehealth using popular video applications like Apple FaceTime, Facebook Messenger video chat, Google Hangouts video, Zoom, and Skype as well as texting applications like Signal, Jabber, Google Hangouts, WhatsApp, iMessage, and Facebook Messenger. However,

healthcare providers were not allowed to use public-facing applications like Facebook Live and Twitch. This change gave providers more options to communicate with low-income population through a smartphone if they did not have a computer or broadband connection.

Relaxing the HIPAA requirements enabled healthcare providers to maintain patient care while protecting populations that might be at a greater risk during the pandemic. Telehealth HIPAA compliance waivers are set to expire when the pandemic ends.

What will happen to telehealth growth after the pandemic?

Growth in telehealth is expected to continue after the pandemic ends because of several factors.

- Even though HIPAA compliance waivers for telehealth are scheduled to expire when the pandemic ends, doctors, healthcare lawyers, and government health officials believe HHS will develop a permanent policy that will continue to encourage telehealth adoption.[6]
- Patient acceptance and demand for telemedicine will continue to grow. Currently, patients must wait weeks or months to make an appointment, miss time from work or school, and travel to and from doctor's offices. Convenience of telehealth will be a big driver of telehealth growth. Moreover, 40% of millennials, the largest segment of the US workforce (83 million), have said that a telehealth option was extremely or very important for them.[7]
- Vast majority of the midsize to large employers offer telehealth benefits to their employees.
- On average, more than 80% of physicians indicated that telehealth enabled them to provide quality care for chronic disease management, and approximately 64% of physicians and healthcare professionals are motivated to increase telehealth usage in their practice in the future.[8]
- Advances in next-generation technologies like artificial intelligence (AI), Internet of Things (IoT), wearables, and telehealth robots will make it easier to use telehealth and improve the quality of patient care.

The expected growth of telehealth will present new challenges to compliance personnel.

Next-generation telehealth technologies and their uses

Next generation of telehealth technologies with ultrafast connectivity will connect a diverse range of medical devices and equipment. These medical devices and equipment will collect and provide real-time data and alert care providers of adverse situations. Providers can add patient notes, write prescriptions, and add other data that pharmacists and other specialists can readily access from their own remote locations.

Wearable technologies can continuously monitor blood pressure, glucose, heart rate, sleep, etc. Some of these wearable technologies like Apple Watch and Fitbit are quite popular already. Integrating data collected from these wearable devices to a patient's electronic health record will help providers monitor patients with chronic conditions and prevent urgent care and emergency department visits. During a telehealth visit, the provider can access the ongoing reading from the patient's wearable to get a better understanding of their situation. In emergencies, the specialists can use the patient's real-time wearable data to advise emergency responders on immediate treatments. Wearables will also help providers remotely monitor their patients at home after a hospital stay or during recovery after a surgery or injury. These capabilities could be particularly beneficial for patients in rural areas where an in-person follow-up visit could require significant travel.

Social distancing and contactless interactions during the pandemic have greatly increased the use of self-service kiosks in clinical settings, pharmacies, and other public locations. Currently, these self-service kiosks are mainly used for booking appointments and bill payments, but in the future, more services could be delivered through these kiosks.

During the pandemic, to reduce the exposure of frontline medical workers to the virus, hospitals started using robots to sanitize hospitals, make deliveries, take temperature and vitals, and monitor patients.[9] Since robots do not need PPE or get sick and can be easily disinfected, they were ideal for the pandemic. Shenzhen Third People's Hospital in China and Circolo Hospital in Varese, Italy, are examples of hospitals that have been using robots to monitor their COVID-19 patients. In the future, these robots will be capable of doing more autonomously.

The pandemic drastically increased the use of AI technologies in medicine. With a surge of patients coming into the emergency room during the pandemic, hospitals had to develop innovate solutions to reduce the wait time and connect patients with the correct healthcare resource. During the pandemic, Mayo Clinic and the state of Rhode Island used the AI-based Diagnostic Robotics triage platform to assign a risk score for each patient based on their answers and then matched the patients with the right healthcare resource.[10] In the future, these AI-based technologies will be able to analyze each patient's individual health history, cross-reference with all the latest research, and suggest appropriate diagnosis and treatment protocols.

Growth in telehealth services will result in an exponential growth in PHI data

Telehealth technologies will continuously generate enormous amounts of protected health information (PHI) data. To function correctly, these technologies will also depend on secure storage and availability of all this PHI data. This data growth will make healthcare data a prime target for hackers and others with malicious intent. Currently, healthcare data are more valuable on the black market because they contain almost all of the personally identifiable information of an individual compared to a financial record, which only contains a single marker. On the black market, a healthcare data record may be valued up to $250 per record compared to the $5.40 for the next highest value record, a payment card.[11]

There have been more healthcare data breaches in 2020 than any other year since records first started being published.[12] In 2020, there has been an average of 1.76 healthcare data breaches per day. Hacker attacks are becoming more and more common in healthcare because of the number of interconnected devices and the need for organizations to share information across multiple devices and third-party vendors. The number of incidents of unauthorized access due to employee errors, negligence, and acts by malicious insiders were also highest in 2020.

In this environment, the addition of newer telehealth technologies will create more vulnerabilities in protecting healthcare data.

Risk of PHI exposure with telehealth technologies

There are two different aspects of privacy and security of patient data in telehealth services. First is ensuring the communication during the telehealth session is safe and secure. Second is ensuring that the patient data are stored securely, and only authorized personnel can access patient records. To comply with HIPAA requirements, healthcare organizations should effectively address both aspects.

For telehealth services to work effectively, multiple technologies and devices need to share PHI data with each other. To seamlessly share data and communicate with each other, each technology/device might have to store

data in multiple locations. In a telehealth technology environment, each data storage point is vulnerable to a hacker attack. The sum of all these vulnerable points is defined as the "attack surface."[13] Risk exposure is less when attack surface is smaller, but telehealth technologies like wearables and IoT will increase the attack surface exponentially.

Wearables and continuous monitoring devices present security concerns by their very nature. Most of the data they generate would be classified as protected data under HIPAA regulations. For example, healthcare organizations need to protect the confidentiality and integrity of the data from a continuous glucose monitoring device as the data arrive and become part of the patient's confidential health record. Using secure connections and data encryption during telehealth sessions can protect PHI.

When delivering telehealth, service providers need to be certain of the identity of the patient. Healthcare organizations can use multifactor authentication and biometrics (fingerprints or facial recognition) to validate the identity of a patient. Including contextual information with an identity management system will improve security of the telehealth system. Contextual information would include the make and model number of a wearable, parental consent for minors, and patient behavior information like when and how they use the system will improve the security. A versatile identity management system that can validate a patient's identity across multiple telehealth systems (single sign-on) will improve the patient experience.

Healthcare organizations should also develop functional and operational privacy policies and processes that protect patient's privacy and data captured during and after the telehealth encounter. Healthcare professionals and the patients should also be trained to develop a privacy mindset. For example, a provider could engage in a secure telehealth session, but if the patient is in an area where unauthorized people can see or hear the interaction, the patient's privacy could be compromised. Training providers and patients on the dos and don'ts of telehealth sessions is one of the best ways to deal with such privacy concerns.

HIPAA compliance best practices for telehealth services

To provide an effective telehealth program, healthcare organizations should develop a comprehensive compliance program that includes risk assessment, management, and mitigation plans along with continuous auditing and monitoring efforts. The following are some of the best practices to develop a telehealth compliance program:

- Ensure that all telehealth applications and technologies meet HIPAA privacy and data security requirements.
- Develop a comprehensive PHI data flow map that identifies how and where PHI data are created and enter the organization, how the data flow through the organization, and how they leave the organization. The data flow map should be kept up to date as processes and technologies evolve.
- Integrate telehealth platforms with the electronic health record system to create a single source of PHI data.
- Ensure all communications and patient data are encrypted and protected.
- Implement a versatile identity management system that is secure and easy to use.
- Establish telehealth policies and processes that protect patient data.
- Train healthcare professionals and patients on dos and don'ts of telehealth program.

The expansion of telehealth services that started during the pandemic will continue to grow in the future. While HIPAA regulations related to telehealth services might change, compliance professionals will need to update themselves on the various risk elements of a telehealth program. A safe and secure telehealth program that protects patient data will greatly improve the adoption of telehealth services and patient health outcomes.

Takeaways

- Telehealth services grew dramatically during the pandemic.
- During the pandemic, the U.S. Department of Health & Human Services issued Health Insurance Portability and Accountability Act (HIPAA) compliance waivers for HIPAA telehealth technologies.
- Telehealth services will continue to grow after the pandemic.
- Protected health information and its exposure risk will grow exponentially with widespread use of telehealth services.
- Healthcare organizations should implement HIPAA compliance best practices for telehealth services.

1 Ateev Mehrotra et al., "The Impact of the COVID-19 Pandemic on Outpatient Visits: Practices Are Adapting to the New Normal", The Commonwealth Fund, June 25, 2020, https://bit.ly/3bvGtTx.
2 "Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency," U.S. Department of Health & Human Services, last reviewed March 30, 2020, http://bit.ly/3danGfP.
3 FAIR Health, "Monthly Telehealth Regional Tracker, Dec. 2020: United States," accessed May 17, 2021, https://bit.ly/3hyVqbj.
4 Ayanna Alexander, "Pandemic Expands Telehealth Despite Privacy Law: HIPAA Explained," Bloomberg Law, May 8, 2020, https://bit.ly/3eTpbSr.
5 "HIPAA flexibility for telehealth technology," Health Resources and Services Administration, Telehealth.HHS.gov, last updated January 28, 2021, https://bit.ly/3hyiCGJ.
6 Ayanna Alexander, "Pandemic Expands Telehealth Despite Privacy Law."
7 Will Rumsey, "29 Statistics You Need To Know About Healthcare & Telemedicine," First Stop Health, February 26, 2021, https://bit.ly/30oMEy2.
8 COVID-19 Healthcare Coalition Telehealth Impact Study Workgroup, "Telehealth Impact: Physician Survey Analysis," November 16, 2020, https://bit.ly/2RiS01Z.
9 Erico Guizzo and Randi Klett, "How Robots Became Essential Workers in the COVID-19 Response," IEEE Spectrum, September 30, 2020, https://bit.ly/2RZM7Xi.
10 Gil Press, "The Future of AI In Post-COVID Healthcare," *Forbes*, March 22, 2021, https://bit.ly/30ovmBc.
11 Ellen Neveux, "Healthcare data: The new prize for hackers," SecureLink, last updated November 19, 2020, https://bit.ly/30ELnTz.
12 "Healthcare Data Breach Statistics," HIPAA Journal, accessed May 17, 2021, https://bit.ly/3bROJxJ.
13 Deloitte, *Securing the promise of virtual healthcare: Addressing cyber risk in a new era of medicine*, accessed May 17, 2021, https://bit.ly/3eXsVSU.